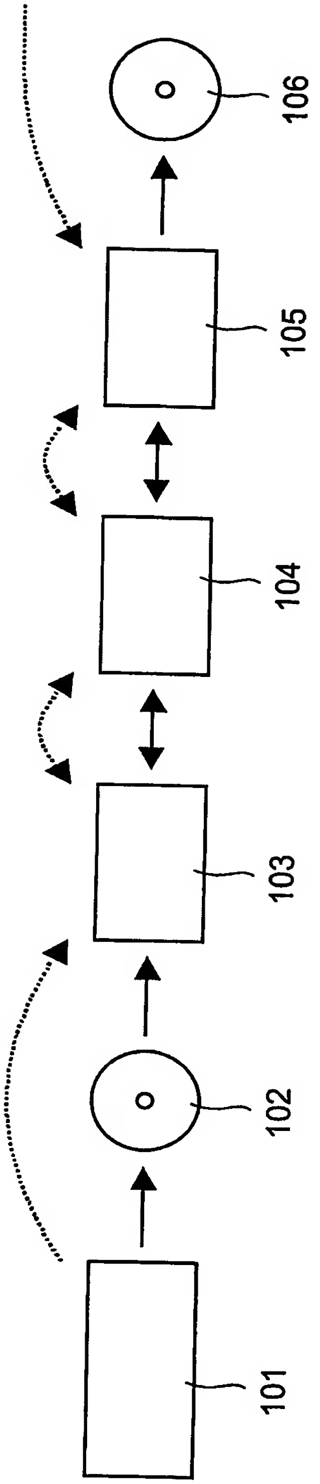

FIG.1

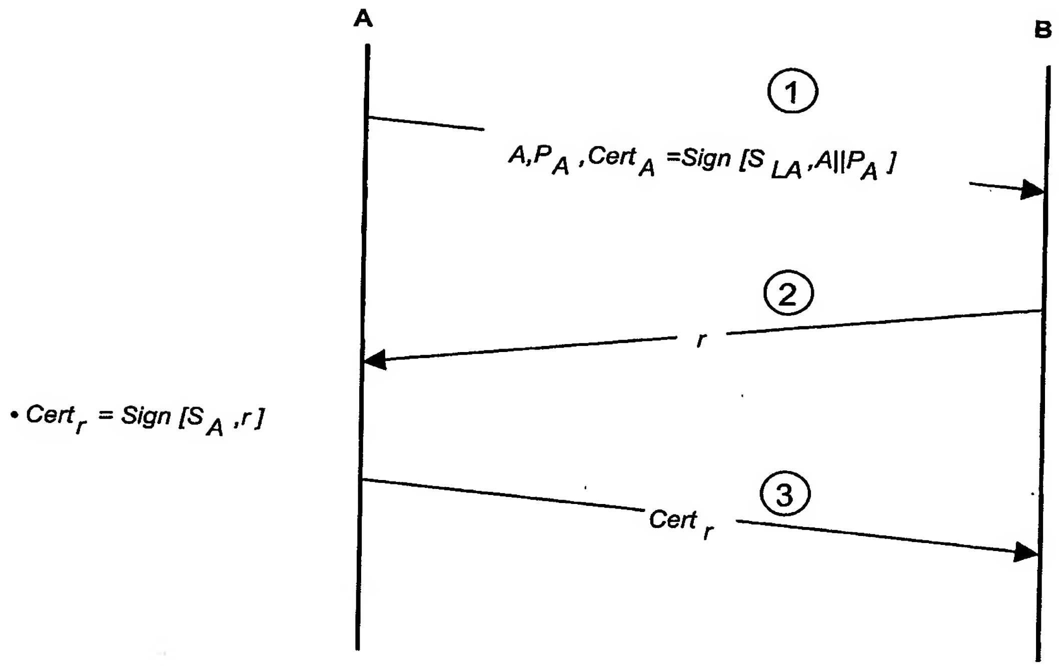
A
B
1
$A, P_A, Cert_A = Sign[S_{LA}, A||P_A]$
2
r
• $Cert_r = Sign[S_A, r]$
3
$Cert_r$

FIG.2

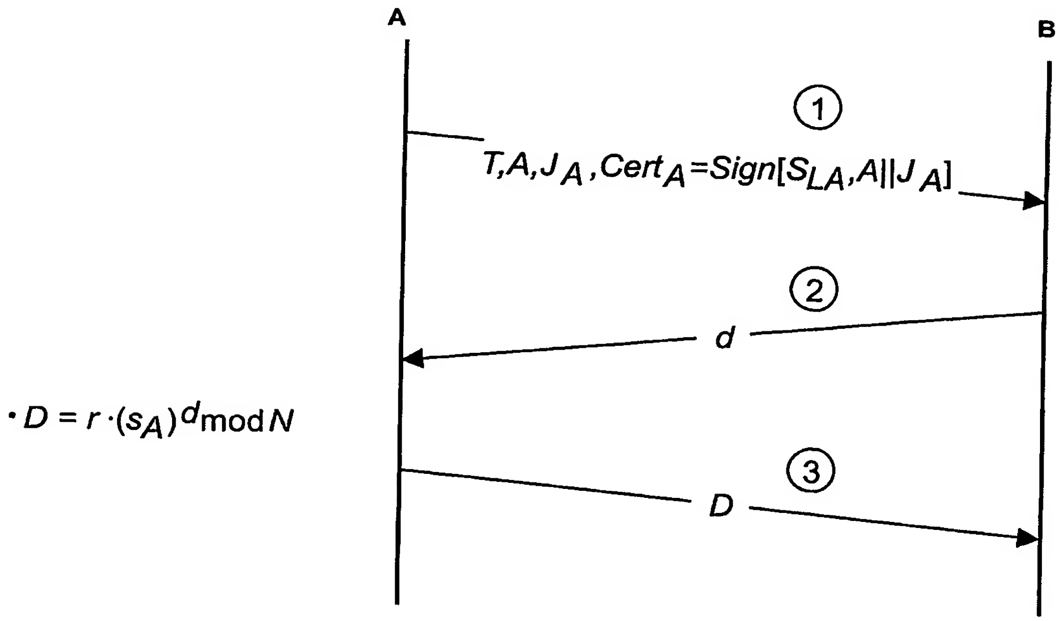
A
B
1
$T, A, J_A, Cert_A = Sign[S_{LA}, A||J_A]$
2
d
$\cdot D = r \cdot (s_A)^d \mathrm{mod} N$
3
D

FIG.3

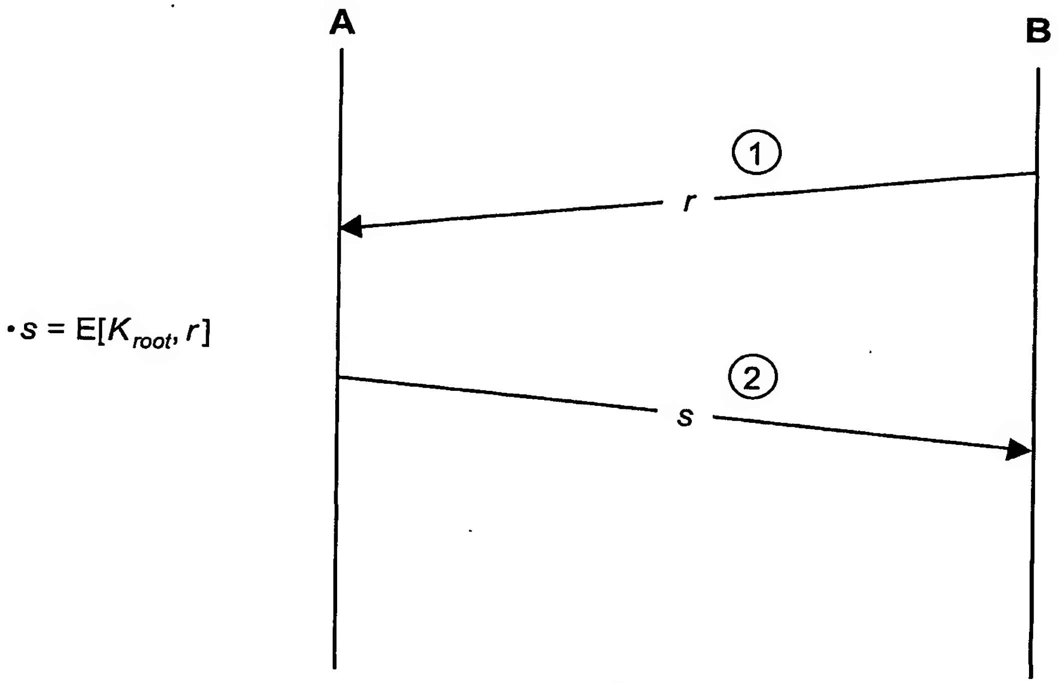

FIG.4

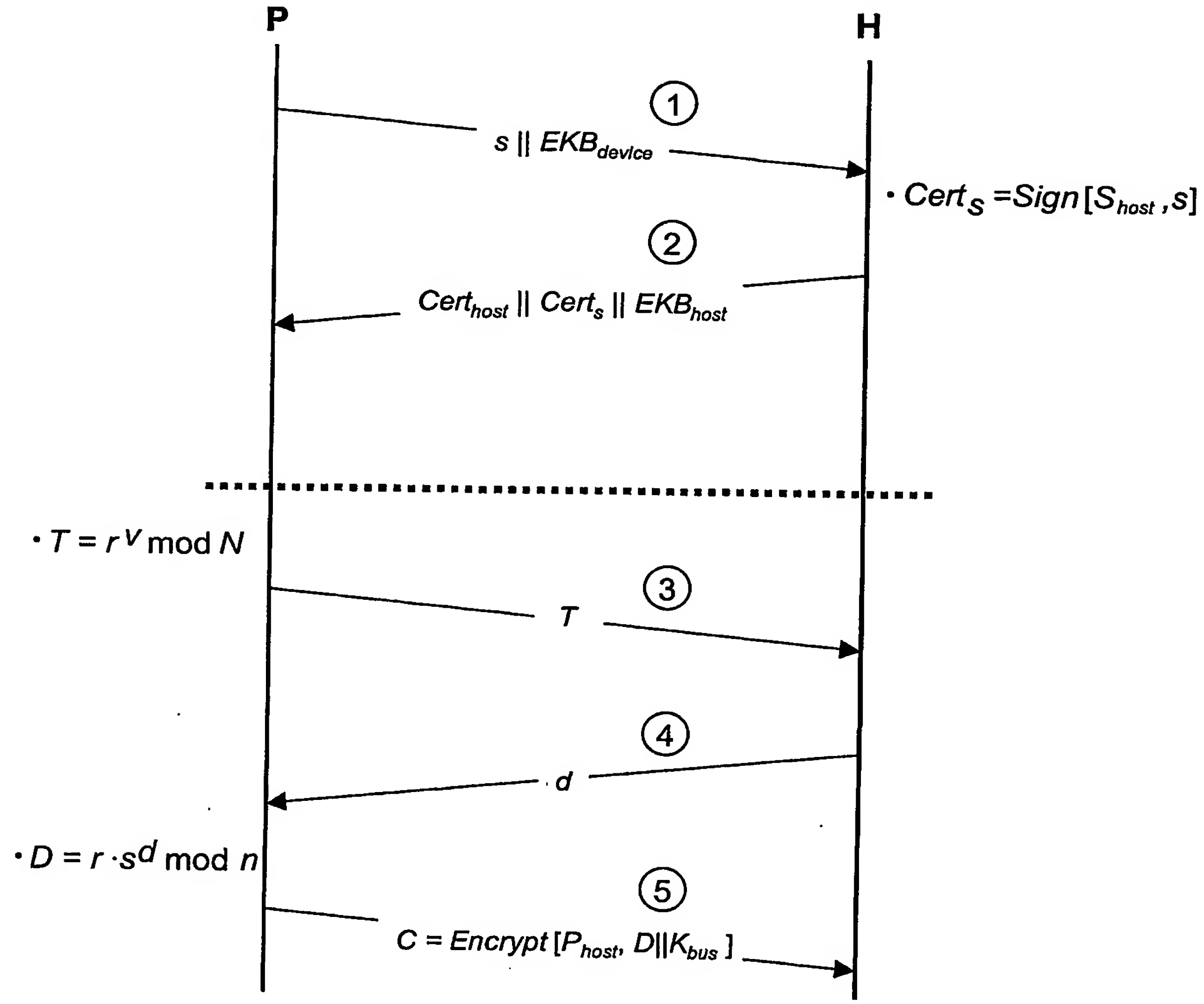
P
H
1
$s \,||\, EKB_{device}$
$\cdot\ Cert_S = Sign[S_{host}, s]$
2
$Cert_{host} \,||\, Cert_s \,||\, EKB_{host}$
$\cdot\ T = r^V \bmod N$
3
T
4
d
$\cdot\ D = r \cdot s^d \bmod n$
5
$C = Encrypt[P_{host}, D||K_{bus}]$

FIG.5

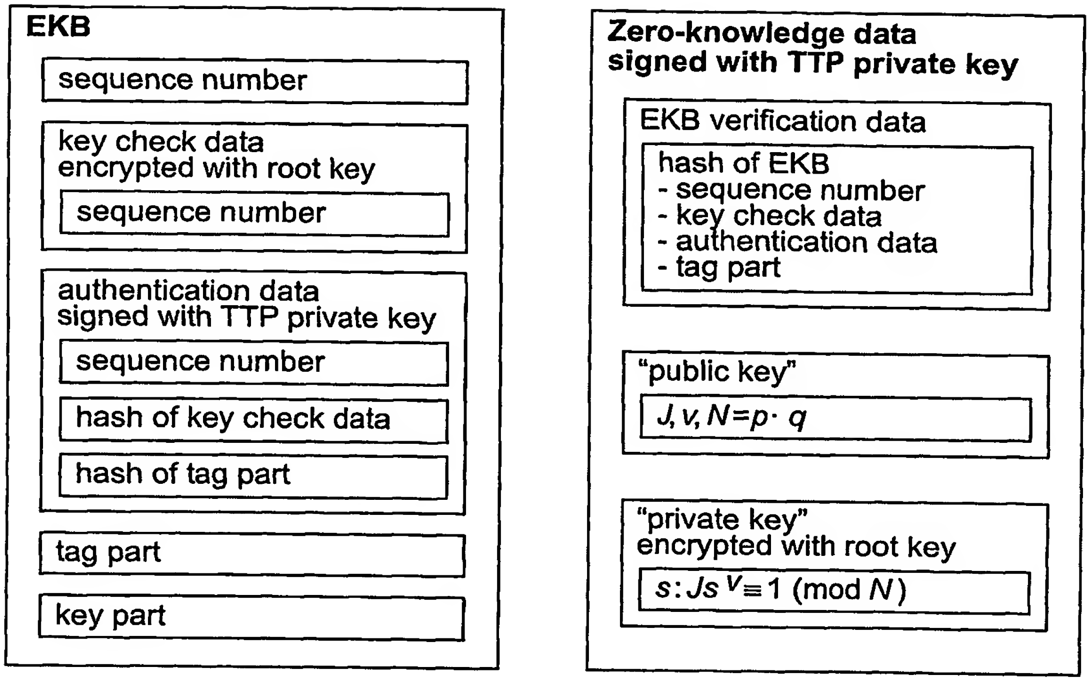
EKB
sequence number
key check data encrypted with root key
sequence number
authentication data signed with TTP private key
sequence number
hash of key check data
hash of tag part
tag part
key part
Zero-knowledge data signed with TTP private key
EKB verification data
hash of EKB
- sequence number
- key check data
- authentication data
- tag part
"public key"
$J, v, N = p \cdot q$
"private key" encrypted with root key
$s: Js^{v} \equiv 1 \pmod{N}$

FIG.6

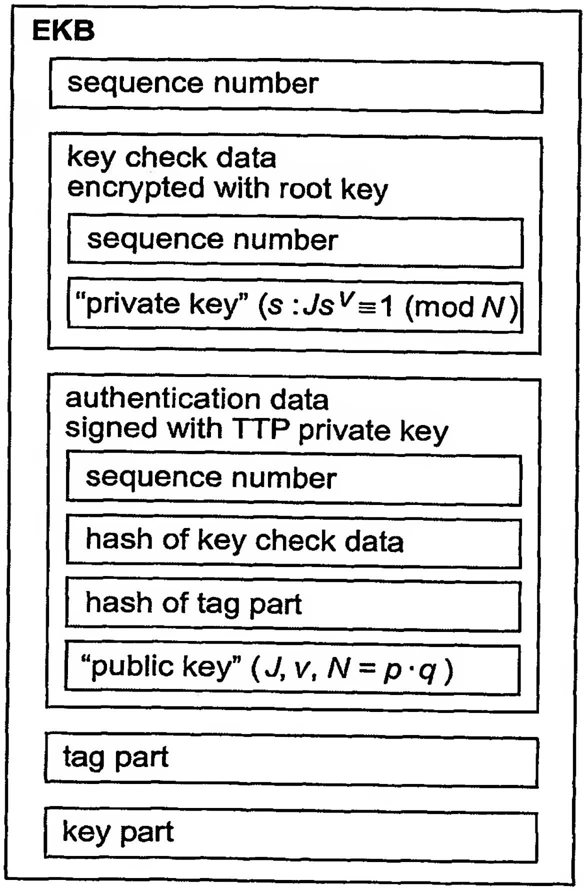
EKB
sequence number
key check data
encrypted with root key
sequence number
"private key" ($s : Js^{v} \equiv 1 \pmod{N}$
authentication data
signed with TTP private key
sequence number
hash of key check data
hash of tag part
"public key" ($J, v, N = p \cdot q$)
tag part
key part

FIG.7